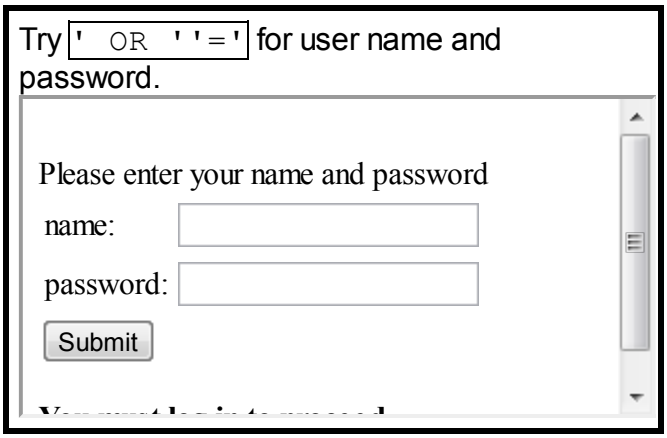
How to exploit the SQL Injection Attack



Exploiting an SQL Inject attack involves solving a puzzle that is a cross between Hangman and 20 Questions. It needs a little understanding of SQL and a great deal of cunning.

Try your Hacking skills against this test system. It takes you through the exploit step-by-step.

The SQL Injection attack allows external users to read details from the database. In a well designed system this will only include data that is available to the public anyway. In a poorly designed system this may allow external users to discover other users' passwords.

Try these steps:

- **To gain access and find a user name.** Enter the string `'OR''='` as both user name and password in the frame on the right. This should get you logged in as a user (jake happens to be the first user in the table). This tells you that Jake is a user and it allows you to access his account - but it does not tell you his password.
- **Find out if Jake's password includes the letter "w".** Enter `xxx` as user name and enter the following string as the password:

```
' OR EXISTS(SELECT * FROM users WHERE name='jake' AND password LIKE '%w%') AND ''='
```

Reset

- **Find out if Jake's password has "w" as the third letter.** Enter `xxx` as user name and enter the following string as the password:

```
' OR EXISTS(SELECT * FROM users WHERE name='jake' AND password LIKE '__w%') AND ''='
```

Reset

Diagnosis
: In which we explain how to identify a web site that may be vulnerable to an SQL Injection attack.

Causes and Cures for SQL Injection Vulnerability
: Explains the programming error that gives rise to the problem.

Exploit: Gain unauthorized Access
: In which we explain how to get past a login screen without knowing a user name or a password.

Exploit: Find a password.
: In which we explain how to discover the password for a user if you know the name of the password table and a user account.

Exploit: Find a user account.
: In which we explain how to discover the user names in the password table given that we know the name of the password table.

Exploit: Find the names of the tables.
: In which we discover the names of the tables available for viewing. this might include the name of the password table.

WARNING: In many countries (including UK) it is illegal to use this attack. I've set up a vulnerable test system here so that you can have a go. I promise not to prosecute.

- Up to 6 months in jail for unauthorised access
- Up to 5 years if with intent to commit further offences
